

UNITED STATES DISTRICT COURT

for the
Southern District of OhioIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

DELL LAPTOP, LATITUDE 2100

Case No.

1:13MJ-603

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A.

located in the Southern District of Ohio, there is now concealed (identify the person or describe the property to be seized):

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
 18 U.S.C. 1029 (a)(8)
 18 U.S.C. 371

Offense Description
 Fraud and related activity in connection with access devices
 Conspiracy to violation section 1029

The application is based on these facts:

See the Affidavit of SA Steven McKenna.

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

Steven McKenna, Special Agent - USSS

Printed name and title

Sworn to before me and signed in my presence.

Date: 10/2/13

Judge's signature

City and state: Cincinnati, Ohio

Karen Litkovitz, U.S. Magistrate Judge

Printed name and title

ATTACHMENT A

The property to be searched is a DELL laptop, Latitude 2100, serial number illegible, the word "Argonne," and the number "24" written in black marker on the lid, hereinafter the "Device." The Device is currently located at the Springdale Police Department, 12105 Lawnview Avenue, Springdale, OH, 45246.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Device described in Attachment A that relate to violations of Title 18 U.S.C Section 1029 and involve Dimitar Angelov and Dimitar Kolev including:

- a. records of credit card account numbers, credit card track information;
- b. All documents, including all temporary and permanent electronic files and records, (including, but not limited to, JPG, GIF, TIF, AVI, WAV and MPEG files) which contain information related to unauthorized access devices, as defined in 18 U.S.C. 1029.
- c. lists of victims and related identifying information;
- d. all bank records, checks, credit card bills, account information, and other financial records.
- e. Electronically stored communications or messages reflecting computer on-line chat sessions or e-mail messages with any persons regarding the possession, receipt, distribution, and/or reproduction of credit card accounts.
- f. Any and all usernames, email accounts, or online identities that may have been used for the unauthorized use of credit cards.

2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as;

- a. evidence of who used, owned, or controlled the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry

entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

- b. evidence of software that would allow others to control the Device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the lack of such malicious software;
- d. evidence of the attachment to the Device of other storage devices or similar containers for electronic evidence;
- e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Device;
- f. evidence of the times the Device was used;
- g. passwords, encryption keys, and other access devices that may be necessary to access the Device;
- h. documentation and manuals that may be necessary to access the Device or to conduct a forensic examination of the Device;
- i. records of or information about Internet Protocol addresses used by the Device;
- j. records of or information about the Device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages,

search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

- k. contextual information necessary to understand the evidence described in this attachment.

.As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO

IN THE MATTER OF THE SEARCH OF A
DELL LAPTOP, LATITUDE 2100,
DESCRIPTION OUTLINED IN
ATTACHMENT A, CURRENTLY
LOCATED AT THE SPRINGDALE POLICE
DEPARTMENT, 12105 LAWNVIEW
AVENUE, SPRINGDALE, OH 45246

Case No. _____

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, Steven W. McKenna, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the United States Secret Service (USSS) and I have been so employed since December of 2004. I have received training on conducting investigations involving violations of federal law. I am currently assigned to the United States Secret Service Cincinnati Field Office and have been assigned to participate in investigations involving violations of federal law. Prior to my employment as a Special Agent in United States Secret Service, I was employed for 3 years as a sworn Uniformed Officer with the United States Secret Service.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

4. The property to be searched is a DELL laptop, Latitude 2100, serial number illegible, the word "Argonne," and the number "24" written in black marker on the lid, hereinafter the "Device." The Device is currently located at the Springdale Police Department, 12105 Lawnview Avenue, Springdale, OH, 45246.

5. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

6. Based on my experience and training, card skimming is a type of scheme in which credit card and bank card information is stolen or "skimmed" at automatic teller machines ("ATMs") in order to defraud credit card companies and banks, often through the creation of duplicate, counterfeit credit cards. ATM skimming schemes often involves the use of certain tools such as a scanning receiver. The scanning receiver, or "skimmer," is a device used to capture and store the victim's credit card information to be transferred and used later by an unauthorized party.

7. Pursuant to 18 U.S.C. § 1029(e)(8), a "scanning receiver" is defined as a "device or apparatus that can be used to intercept a wire or electronic communication in violation of chapter 119 or to intercept an electronic serial number, mobile identification number, or other identifier of any telecommunications service, equipment, or instrument."

8. On September, 28 2013, Springdale (OH) Police Officers responded to a call of service of two suspicious individuals, in a white Toyota Corolla, IL tag#L388215, in the parking lot located at 175 Tri-County Parkway, Springdale, Ohio. The caller stated the two subjects parked on the far side of the building, hung around for several minutes adjusting their jackets. One of the subjects crossed the street, walked past 175 Tri-County Parkway, crossed back across the street to the lot of Kemba Credit Union located at 211 Northland Blvd, and went to the ATM. The subject then returned to the Corolla in the same manner. Once he returned, they hung around for several more minutes, adjusting their jackets and the other male subject walked to the ATM in the same manner. They drove off just before officers arrived.

9. Officer Abell spotted the vehicle leaving the parking lot located at 200 Northland Blvd, Springdale, OH, which is across the street from the Kemba Credit Union, heading back towards Tri-County Parkway. Officer Warren and Sgt. Davis stopped the vehicle on SR 747 as it pulled into the parking lot of Cassanelli Square.

10. As the stop was made, both occupants took items off their heads. The driver took off a wig and sunglasses, throwing the wig into rear seat. The passenger took off a hat and threw it into the rear seat.

11. Officers approached the vehicle and spoke with the driver, who provided an IL ID with name Dimitar Angelov ANGELOV. The passenger provided an IL OL under the name Dimitar KOLEV.

12. The officers observed a strong odor of marijuana emanating from the passenger compartment of the vehicle.

13. ANGELOV was asked about what he was doing on Tri-County Parkway. He stated they were just hanging out. When asked about Kemba and the ATM, they denied going anywhere near an ATM, and again said they were just hanging out. ANGELOV stated they were from Chicago and were headed back to Chicago. When asked what they were doing in Cincinnati, he replied they were looking to purchase a truck. When asked about the marijuana, he stated that they do use marijuana. When asked if they had any in the car, he said yes, and showed a folded piece of paper with some residue on it. When asked if they had anymore, he replied no. ANGELOV stated "in Chicago they were allowed to have up to an ounce without any problem."

14. ANGELOV then gave consent to Officer Warren to search the vehicle. Both men were removed from the vehicle and placed into patrol cars. During the search of the vehicle, a baggie containing a small amount of marijuana was found in the center console, along with other baggies and paper with marijuana residue. Some paraphernalia was also found in a cubby hole in the center dash.

15. During the search, numerous prepaid credit cards and other similar cards with electronic information strips were found. Some of the cards had masking tape on the back of the card with hand written four digit numbers on the tape. Officers also observed 2 laptop computers and numerous electronic cords, one of which was rigged with alligator clips and "pig tail" wires. The car was towed to the Springdale Police department.

16. A representative from Kemba Credit Union was contacted and responded to the bank's ATM at Kemba. The ATM was examined and a skimming device was located on the card slot of the machine. There was also a device located over the cash dispenser that appeared to have a camera in it. This device was also equipped with a USB cable.

17. Surveillance video photos were obtained and examined from Kemba Credit Union. The photo depicts a subject wearing a coat, similar to the coat worn by Dimitar Angelov ANGELOV at the time of the traffic stop, at the ATM. The photos also showed another subject wearing a coat that matched a coat that was lying in the rear seat of the car.

18. A Hamilton County (OH) Municipal Court Search Warrant was signed and executed on the white Toyota Corolla, bearing IL tag#L388215.

19. Inside the Toyota Corolla, items were recovered that are consistent with items that individuals use who conduct access device fraud. Among these items: a skimming device artificially attached to a piece of an ATM, a circuit board (similar to the one found at the Kemba Credit Union), a blue Toshiba lap top computer (S# 1A062958Q), a yellow Dell lap top computer (illegible S#, Model Latitude 2100), numerous prepaid credit/gift cards (some of which contained masking tape with had written four digit numbers on the back), a soldering iron (wire), pry bar, box cutter, gloves and a wig.

20. Based upon my experience and training, individuals who engage in access device fraud transfer victim's credit card data that is obtained from the skimming device to computers for better access. There is probable cause to believe that the Device found in ANGELOV's vehicle contains evidence of access device fraud.

21. The Device is currently in the lawful possession of the Springdale Police Department. It came into the Springdale Police Department's possession in the following way: A Hamilton County (OH) Municipal Court Search Warrant was signed and executed on the white Toyota Corolla, bearing IL tag#L388215. The Device was recovered in the passenger compartment of the vehicle. Therefore, while the Springdale Police Department might already

have all necessary authority to examine the Device, I seek this additional warrant out of an abundance of caution to be certain that an examination of the Device will comply with the Fourth Amendment and other applicable laws.

22. The Device is currently in storage at 12105 Lawnview Avenue, Springdale, OH, 45246. In my training and experience, I know that the Device has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Device first came into the possession of the Springdale Police Department.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

23. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

24. There is probable cause to believe that things that were once stored on the Device may still be stored there, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file

on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

25. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used,

the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

- d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.
- f. I know that when an individual uses an electronic device to obtain unauthorized access to a victim electronic device over the Internet, the individual's electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain: data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

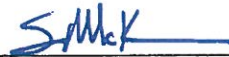
26. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

27. Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

28. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,



Steven W. McKenna
Special Agent
U.S. Secret Service

KU Subscribed and sworn to before me
on October 2, 2013:



UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

The property to be searched is a DELL laptop, Latitude 2100, serial number illegible, the word "Argonne," and the number "24" written in black marker on the lid, hereinafter the "Device." The Device is currently located at the Springdale Police Department, 12105 Lawnview Avenue, Springdale, OH, 45246.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Device described in Attachment A that relate to violations of Title 18 U.S.C Section 1029 and involve Dimitar Angelov and Dimitar Kolev including:
 - a. records of credit card account numbers, credit card track information;
 - b. All documents, including all temporary and permanent electronic files and records, (including, but not limited to, JPG, GIF, TIF, AVI, WAV and MPEG files) which contain information related to unauthorized access devices, as defined in 18 U.S.C. 1029.
 - c. lists of victims and related identifying information;
 - d. all bank records, checks, credit card bills, account information, and other financial records.
 - e. Electronically stored communications or messages reflecting computer on-line chat sessions or e-mail messages with any persons regarding the possession, receipt, distribution, and/or reproduction of credit card accounts.
 - f. Any and all usernames, email accounts, or online identities that may have been used for the unauthorized use of credit cards.
2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as;
 - a. evidence of who used, owned, or controlled the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry

entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

- b. evidence of software that would allow others to control the Device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the lack of such malicious software;
- d. evidence of the attachment to the Device of other storage devices or similar containers for electronic evidence;
- e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Device;
- f. evidence of the times the Device was used;
- g. passwords, encryption keys, and other access devices that may be necessary to access the Device;
- h. documentation and manuals that may be necessary to access the Device or to conduct a forensic examination of the Device;
- i. records of or information about Internet Protocol addresses used by the Device;
- j. records of or information about the Device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages,

search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

- k. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.